

**REDACTED
COPY**

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF TEXAS
SAN ANTONIO DIVISION

FILED

May 19, 2021

CLERK, U.S. DISTRICT COURT
WESTERN DISTRICT OF TEXAS

BY: MGR
DEPUTY

UNITED STATES OF AMERICA,
Plaintiff,

v.

OLUFEMI NATHANIEL ITIOWE. (1)
a/k/a Baloi Maputo Oldemiro
and John Koffi
STACEY ALLISON AULT. (2)
a/k/a Tammy Botha
and Cindy Theron
ENSO J. ANDERSON. (3)

[REDACTED]

Defendants.

SEALED INDICTMENT

SA-21-CR-224-FB

SA-21-CR-_____

[VIOLATION:


Count One: 18 U.S.C. § 1956 (h);
Conspiracy to Commit Money Laundering

**Notice of Government's Demand
for Forfeiture.]**

THE GRAND JURY CHARGES THAT:

COUNT ONE
(18 U.S.C. § 1956 (h))

Beginning on or about October 5, 2018 and continuing through and including on or about September 17, 2019, in the Western District of Texas, the Northern District of Texas, the Eastern District of New York, the Southern District of New York, the District of New Jersey, the Eastern District of North Carolina, the Middle District of North Carolina, the Eastern District of Missouri, the Western District of Oklahoma, the District of Montana, the District of Nevada, the Northern District of California and elsewhere, the defendants,

OLUFEMI NATHANIEL ITIOWE, a/k/a Baloi Maputo Oldemiro and John Koffi,
STACEY ALLISON AULT, a/k/a Tammy Botha and Cindy Theron,
ENSO ANDERSON,


did knowingly conspire, confederate, and agree with each other and with other persons known and unknown to the Grand Jury to commit offenses against the United States, that is, to violate Title 18, United States Code, Sections 1956 and Section 1957; to wit:

(a) to knowingly conduct and attempt to conduct a financial transaction affecting interstate and foreign commerce, which involved the proceeds of a specified unlawful activity, specifically, *Wire Fraud*, in violation of Title 18, United States Code, section 1343, with the intent to promote the carrying on of a specified unlawful activity, specifically *Wire Fraud* in violation of Title 18, United States Code, section 1343, and that while conducting and attempting to conduct such financial transaction knew that the property involved in the financial transaction represented the proceeds of some form of that specified unlawful activity in violation of Title 18, United States Code, Section 1956(a)(1)(A)(i):

(b) to knowingly conduct and attempt to conduct financial transactions affecting interstate commerce and foreign commerce, which transactions involved the proceeds of specified unlawful activity, specifically *Wire Fraud* in violation of Title 18, United States Code, section 1343, knowing that the transactions were designed in whole or in part to conceal and disguise the nature, location, source, ownership, and control of the proceeds of said specified unlawful activity, and that while conducting and attempting to conduct such financial transactions, knew that the property involved in the financial transactions represented the proceeds of said unlawful activity, in violation of Title 18, United States Code, Section 1956(a)(1)(B)(I):

(c) to transport, transmit and transfer and attempt to transport, transmit and transfer a

Case 1:21-mj-00676-RLM Document 1 Filed 06/09/21 Page 10 of 25 PageID #: 10

monetary instrument and funds from a place in the United States to and through a place outside the United States with the intent to promote the carrying on of specified unlawful activity, that is, Title 18, United States Code, section 1343, *Wire Fraud* in violation of Title 18, United States Code, Section 1956(a)(2)(A); and

(d) to knowingly engage and attempt to engage, in monetary transactions by, through or to a financial institution, affecting interstate and foreign commerce, in criminally derived property of a value greater than \$10,000, such property having been derived from a specified unlawful activity, that is, Title 18, United States Code, section 1343, *Wire Fraud* in violation of Title 18, United States Code, Section 1957.

Background

At all times material to the Indictment:

1. A “business email compromise” (BEC) is a type of computer intrusion to a business email system that compromises one or more email addresses used by employees for business purposes. Once a criminal actor has gained access and control of an employee’s email account, the actor will monitor the employee’s email activity, or in some instances, establish email rules within the email application that will divert all of the employee’s emails, or only emails that meet certain criteria for later review. The criminal actor is typically looking for emails dealing with financial transactions, to include business to business payments, the purchase of property or, matters involving investments.

2. In one common BEC scheme, the criminal actor monitors incoming and outgoing email messages to determine when a large financial transaction is scheduled to take place. After initial transfer or wiring instructions are conveyed between legitimate parties to the transaction,

the intruder sends a phony follow-up email that appears to be coming from the original legitimate sender. This “spoofed” email contains a change of plans, instructing that the money to be wired instead go to a different account - one that is controlled by the criminal actor, or a conspirator of the criminal actor, and that is set up for the purpose of receiving and redirecting funds acquired illegally from the BEC scheme.

3. The fraudulent banking information is most often connected with individuals who willingly take part in laundering the money from their bank accounts to another bank account owned or under the control of the criminal actor, or conspirators. Conspirators, acting in concert with the criminal actors behind the BEC attack, may include people known as “Money-Mules.” These Money-Mules act on behalf of the criminal actors behind the BEC attack to move and divert the stolen money as many times as possible in the shortest period of time.

4. Similar to a BEC computer intrusion, a criminal actor can also target an individual’s personal email system and compromise one or more email addresses used by an individual for their personal purposes. Once a criminal actor has gained access and control of an individual’s email account, the actor will monitor the email activity, or in some instances, establish email rules within the email application that will divert all of the individual’s emails, or only emails that meet certain criteria for later review. The criminal actor is typically looking for emails dealing with financial transactions, to include business to business payments, the purchase of property or, matters involving investments.

The Scheme to Defraud

5. The Defendants, **OLUFEMI NATHANIEL ITIOWE**, a/k/a Baloi Maputo Oldemiro and John Koffi, **STACEY ALLISON AULT**, a/k/a Tammy Botha and Cindy Theron,

ENSO ANDERSON, [REDACTED] and others known and unknown to the Grand Jury, were conspirators and associates of the criminal actors involved in BEC attacks on businesses and individuals located in the Western District of Texas and elsewhere. These conspirators and associates functioned as a continuing unit for a common purpose of achieving the objectives of the conspiracy. The conspiracy and its activities affected, interstate and foreign commerce.

6. The conspiracy, which operated in the Western District of Texas and elsewhere in the United States, operated through groups of individuals responsible for the various fraudulent schemes and criminal activities conducted by the conspirators.

7. The principal purpose of the conspiracy was to generate money for its conspirators and associates. This purpose was implemented by conspirators and associates committing various criminal acts, including wire fraud, and money laundering.

8. The conspirators and associates sought, among other things, to:

- a. Preserve and protect the ability of the conspiracy to enrich its conspirators and associates through the corrupt use of false and fictitious identities to hinder detection by law enforcement; and
- b. Promote and enhance the criminal activities of the conspiracy and its conspirators and associates.

9. The conspiracy was bound together by, among other things, the conspirators' and associates' common interest, knowledge, and usage of email communications and its vulnerabilities to fraudulently obtain money from victims pursuant to various fraudulent schemes, including but not limited to, a scheme to divert and steal money from businesses and individuals

by creating and sending fictitious emails that appeared to be coming from an original legitimate sender but contained instructions that the money to be wired instead go to an account controlled by the criminal actor, conspirators and associates.

10. For the common purpose of generating criminal proceeds and for the personal enrichment of the conspirators and associates through the conduct of the above-listed criminal activities, at various times relevant to this Indictment, conspirators and associates engaged in:

- a. fraudulently inducing victims to send money to bank accounts controlled by the criminal actor, or conspirators;
- b. making false and fraudulent representations to banks and creating false documents;
and
- c. using individuals to withdraw funds from conspirator and/or associate controlled accounts or pick up or transfer funds using money transfer services.

Manner and Means

11. The defendants and others known and unknown to the Grand Jury, accomplished, and attempted to accomplish the objectives of the conspiracy including but not limited to, the following:

12. Unindicted coconspirators, using computers and the Internet, performed computer intrusions into business email systems and email systems belonging to individuals. These computer intrusions compromised one or more email addresses used by business employees and compromised the email addresses of individual used for personal use.

13. Unindicted conspirators would monitor an employee's email account and employee's email activity, or an individual's personal email account and email activity once the unindicted conspirator had access to and control of the email accounts.

14. Unindicted conspirators, in some instances, created and established email rules within the business' email program or personal email account that would redirect the employee's or individual's emails to the unindicted conspirator for subsequent review. Other established email rules created by the unindicted conspirator acquired business emails or an individual's emails that met certain criteria for later review. In these diverted emails, the unindicted conspirator looked for information concerning financial transactions, to include business to business payments, the purchase of property or matters involving investments.

15. When a diverted email identified that a large financial transaction was scheduled to take place, an unindicted conspirator would direct and send an email message that appeared to be from the original legitimate sender. The unindicted conspirator conveyed additional or new instructions, directing that the money involved in the transaction be wired or transmitted electronically to a different account - one controlled by the unindicted conspirator or other conspirators acting together.

16. The defendants, other unindicted coconspirators, and others known and unknown to the Grand Jury, communicated with each other to provide timely notice of the arrival of a victim's wire transfer of funds into one of the bank accounts they controlled. The defendants, other unindicted coconspirators, and others known and unknown to the Grand Jury, quickly withdrew the victim's diverted proceeds from these accounts and distributed the proceeds to promote the scheme, and for their own personal enrichment.

17. To avoid detection from law enforcement and the victims, the defendants, other unindicted coconspirators, and others known and unknown to the Grand Jury created false identification documents, fictitious businesses, and opened bank accounts using aliases and assumed names.

18. The defendants, other unindicted coconspirators, and others known and unknown to the Grand Jury collected the victim's diverted money in a variety of ways, including physically appearing at banking institutions throughout the United States to withdraw the targeted proceeds or to structure withdrawals of proceeds. The defendants, other unindicted coconspirators, and others known and unknown to the Grand Jury delivered the victim's diverted money to other conspirators and their associates, or made arrangements to wire transfer the funds to bank accounts in the names of other conspirators and associates.

19. The victim's diverted money received by the defendants, other unindicted coconspirators, and others known and unknown to the Grand Jury was laundered to promote the email compromise conspiracy, perpetuate the conspiracy, conceal and disguise the proceeds obtained from victims of the email compromise, promote its fraudulent affairs, and for the personal enrichment of the defendants.

The defendants, co-conspirators, and others engaged in various financial transactions, including but not limited to:

20. Victim P&C:

- a. On or about May 9, 2019, a company referred to herein as "Victim P&C", located in San Antonio, Texas, in the Western District of Texas, became the victim of a BEC fraud totaling over \$300,000. In May 2019, Victim-P&C was awaiting the

deposit of funds from a San Antonio, Texas based money management company.

On or about May 8, 2019, the money management company received an email appearing to be from an employee of Victim-P&C, however, in reality, it was a spoofed email address from defendants, unindicted co-conspirators, or others executing a BEC fraud scheme. The spoofed email contained fraudulent wiring instructions directing the money management company to transfer the funds to accounts owned or under the control of defendant **ENSO ANDERSON** and an unindicted co-conspirator. Neither **ANDERSON** nor the unindicted co-conspirator were legitimate parties to the Victim-P&C transaction.

- b. Based on the fraudulent wiring instructions, the money management company wired the funds in two separate wire transfers. It sent one wire transfer for approximately \$138,000 from a bank in Texas to a bank account located in Pennsylvania controlled by an unindicted co-conspirator and another wire transfer from a bank in Texas for \$207,000 to a bank account located in New Jersey controlled by **ANDERSON**.
- c. On or about May 9, 2019, **ANDERSON** withdrew approximately \$150,000 of Victim-P&C's \$207,000. **ANDERSON** then purchased three separate cashier's checks each for approximately \$50,000.
- d. **ANDERSON** made one of the \$50,000 cashier's checks payable to **STACEY ALLISON AULT's** alias identity, Tammy Botha. On or about May 9, 2019, **AULT** or an unknown co-conspirator deposited that Cashier's check into a bank

account owned by **AULT** under the alias "Tammy Botha". On or about May 13, 2019, **AULT** withdrew approximately \$50,000 in cash from this Bank account.

- e. **ANDERSON** made the two other cashier's checks for approximately \$50,000 each payable to **OLUFEMI NATHANIEL ITIOWE**'s alias identity, Baloi Maputo Oldemiro. On or about May 9, 2019, **ITIOWE**, or a co-conspirator operating on his behalf, cashed both checks at a bank located in New York City, New York.

21. **Victim G.E.**

- a. On or about May 15, 2019, a company referred to herein as Victim G.E., a business located in Helena, Montana, was the victim of BEC fraud in which one of its employees intended to pay an invoice to a subcontractor, but was deceived by a spoofed email from the defendants, unindicted co-conspirators, or others who provided fraudulent wiring instruction, into sending over \$600,000 through an interstate wire transfer from a bank in New York, New York to an account controlled by [REDACTED], located in Las Vegas, Nevada, who was not a legitimate party to the intended Victim G.E. transaction.
- b. On or about May 16-17, 2019, using the funds she received from Victim G.E., [REDACTED] purchased cashier's checks that she made payable to:
 - i. Oldemiro General Contractor, Inc., a business established and controlled by **OLUFEMI NATHANIEL ITIOWE** using his alias identity Baloi Oldemiro, for approximately \$99,000, which **ITIOWE** subsequently withdrew on or about May 23-28, 2019;

- ii. STACEY ALLISON AULT's alias identity, Tammy Botha, for approximately \$150,000, which AULT subsequently withdrew on or about May 22-23, 2019.
- iii. [REDACTED], for at least \$125,000, which [REDACTED] subsequently negotiated on or about May 16-17, 2019.

All in violation of Title 18, United States Code, Section 1956(h).

NOTICE OF UNITED STATES OF AMERICA'S DEMAND FOR FORFEITURE
[See Fed.R.Crim.P. 32.2]

This Notice of Demand for Forfeiture includes but is not limited to the property described in Paragraph II.

I.

Money Laundering Conspiracy Violations and Forfeiture Statutes

[Title 18 U.S.C. § 1956(h), subject to forfeiture pursuant to Title 18 U.S.C. § 982(a)(1)]

As a result of the criminal violations set forth in Count One, the United States gives notice to the Defendants of its intent to seek the forfeiture of the money judgment described below upon conviction pursuant to Fed. R. Crim. P. 32.2 and Title 18 U.S.C. § 982(a)(1), which states:

Title 18 U.S.C. § 982.

(a)(1) The court, in imposing sentence on a person convicted of an offense in violation of section 1956, 1957, ... of this title, shall order that the person forfeit to the United States any property, real or personal, involved in such offense, or any property traceable to such property.

II.

Money Judgment

A sum of money which represents the real or personal property involved in or traceable to the violations set forth in Count One referenced above, for which each Defendant is solely liable.

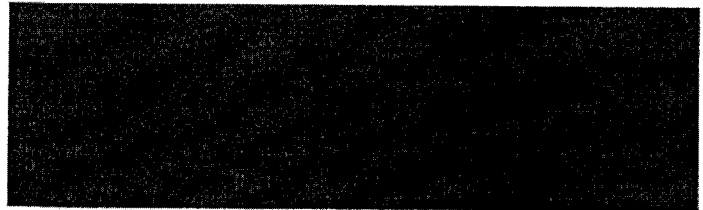
Substitute Assets

If any of the property described above as a result of any act or omission of Defendants:

- a. cannot be located upon the exercise of due diligence;
- b. has been transferred or sold to, or deposited with, a third party;
- c. has been placed beyond the jurisdiction of the court;
- d. has been substantially diminished in value; or
- e. has been commingled with other property which cannot be divided without difficulty;

it is the intent of the United States to seek forfeiture of any other property owned by the Defendants up to the value of the Money Judgment as substitute assets pursuant to Title 21 U.S.C § 853(p) and Fed. R. Crim. P. 32.2(e)(1).

A TRUE BILL.



ASHLEY C. HOFF
UNITED STATES ATTORNEY

BY:

Assistant U.S. Attorney